Chapter 1

The ABCs of GRC

In This Chapter

- Getting to know GRC
- Discovering the GRC stakeholders
- Understanding GRC by the letters
- Deciding on your approach to GRC

Governance, Risk, and Compliance, almost always referred to as GRC, is the latest addition to the parade of three-letter acronyms that are used to describe the processes and software that run the business world. The goal of GRC is to help a company efficiently put policies and controls in place to address all its compliance obligations while at the same time gathering information that helps proactively run the business. Done properly, GRC creates a central nervous system that helps you manage your business more effectively. You also derive a competitive advantage from understanding risks and choosing opportunities wisely. In other words, GRC helps you make sure that you do things the right way: It keeps track of what you are doing and raises an alert when things start to go off track or when risks appear.

This opening chapter takes you on a top-to-bottom tour of GRC to help you understand in greater detail what GRC means and what companies are doing to lower the costs and create new value.

Getting to Know GRC

GRC is not just about complying with requirements for one quarter or one year. Rather, those who are serious about GRC, meaning just about everyone these days, seek to create a system and culture so that compliance with external regulations, enforcement of internal policies, and risk management are automated as much as possible and can evolve in an orderly fashion as business and compliance needs change. That's why some would say that the C in GRC should stand for controls: controls that help make the process of compliance orderly and make process monitoring — and improvement — easier.

Some parts of the domain of GRC — measures to prevent financial fraud, for example — are as old as business itself. Making sure that money isn't leaking out of a company and ensuring that financial reports are accurate have always been key goals in most businesses—only recently have they attained new urgency.

Other parts of GRC related to trade compliance, risk management, and environmental, health, and safety regulations are somewhat newer activities that have become more important because of globalization, security concerns, and increased need to find and mitigate risks. For example, to ship goods overseas, you must know that the recipient is not on a list of prohibited companies. These lists change daily. Growing concern about global warming and other pressures to reduce environmental impact and use energy efficiently have increased regulations that demand reporting, tracking, and other forms of sociopolitical compliance. Companies are also interested in sustainability reporting, measuring areas such as diversity in the workplace, the number of employees who volunteer, and environmental efforts, so that companies can provide data about corporate social responsibility. Financial markets punish companies that report unexpected bad news due to poor risk management.

One simple goal of GRC is to keep the CFO out of jail, but that description is too narrow to capture all of the activity that falls under the umbrella of GRC. (It's also an exaggeration; the truth is that simple noncompliance is more likely to result in big fines rather than a long trip to the big house. But, that said, most executives prefer to leave no stone unturned rather than risk breaking rocks in the hot sun.) Most companies now face demands from regulators, shareholders, and other stakeholders. Financial regulations like Sarbanes-Oxley (SOX) in the United States and similar laws around the world mean that senior executives could face criminal penalties if financial reports have material errors. (For more on Sarbanes-Oxley, flip ahead to Chapter 4.) All of this means a lot more testing and checking, which is costly without some form of automation.

If GRC seems like a sideshow to your main business, remember you can't get out of it, so you might as well make it work for you, not against you. At first, especially in 2004 — the first year in which Sarbanes-Oxley compliance became mandatory — companies frequently engaged in a mad rush, throwing people, auditors, spreadsheets, and whatever resources were required at the problem. Although the rush to comply was heroic, it was far from efficient. Now companies are understanding how to turn GRC activities into an advantage.

The question every company must answer is the following: Will we do the bare minimum to make sure that we stay out of trouble, or can GRC become an opportunity for us to find new ways of running our business better?

Because it is concerned with creating a sustained stream of high-quality information about a business, GRC has a large overlap with Corporate Performance Management (CPM), a topic we cover in greater detail in Chapter 15.

If the burdens of GRC are a cloud, the silver lining is that in learning how to keep track of business in greater depth, GRC activities are transformed from an annoyance to a gateway to an expanded consciousness in a company, which can lead to better performance, reduced costs, and competitive advantage. GRC is part of the natural process of turning strategy into action, monitoring performance, and tracking and managing the risks involved. Choosing to see GRC as an opportunity can mean significant savings in auditing costs, creating new sources of information for improving processes, finding risks earlier, and most of all, avoiding those nasty surprises that spark a punishing reaction in the stock market.

Getting in the Business Drivers' Seat

In some ways, GRC is nothing new: Almost every activity under the bailiwick of GRC has been going on for quite some time in the business world. The segregation of duties that is required by Section 404 of Sarbanes-Oxley has always been part of an auditor's toolkit of recommendations when it comes to preventing fraud. Companies have always been under the obligation to report financial results accurately, to comply and report on their performance with respect to environmental, safety, and trade laws, and to identify risks as early as possible. Every well-run company — whether private or public — puts its own unique self-inflicted policies in place and makes sure that they are being followed. As times change, all of these measures must be updated.

What caused the birth of GRC as an area of focus for companies and those who provide consulting services and software was a perfect storm of urgency about various issues. Consider the following elements of that perfect storm:

- In the wake of the go-go culture of the Internet investing boom of the late 1990s, massive, systematic fraud was revealed at major companies such as Enron, WorldCom, Adelphi, and others. In many cases, the controls and external forms of scrutiny that were in place to stop such bad behavior had failed for many different reasons, including fraud, conflicts of interest, and other forms of malfeasance.
- At the same time, the terrorist attacks on September 11, 2001 led to a worldwide tightening of controls on trade, especially with respect to sales of certain types of products or materials that were deemed dangerous if fallen into the wrong hands. For example, ITT shipped night vision goggle components to China and other countries, resulting in a U.S. Department of Justice fine of $100 million.

- The third force driving the urgency of GRC is the rising concern about energy consumption and the environment. Instability in the Mideast, scarcity of oil supply due to increased consumption, and lack of new oil discoveries have driven oil prices to record highs. Worries about global warming have caused a new wave of demands for energy efficiency, reductions in environmental impact, and a desire for companies to demonstrate the long-term sustainability of their operations.

Lawmakers around the world awoke to this crisis and felt a burning need to DO SOMETHING! A debate still rages about the wisdom of the governmental response, but there is no mistaking the result: an across-the-board increase of the volume and urgency of compliance activities. But seeing GRC only in terms of Sarbanes-Oxley and financial compliance is a mistake. Although complying with Sarbanes-Oxley and other similar laws that have been enacted worldwide certainly spurred many companies to action, after they got started, companies realized that there was a whole other field of compliance, risk, and governance-related activities that needed to be performed with greater attention and efficiency.

Investors, along with governments and regulators, insurance companies, ratings agencies, and activist stakeholders have also joined in increasing the urgency with respect to transparency and accuracy of information about the company's operations and actions taken to mitigate risks and issues. Stock markets have dealt brutal punishment to companies that report problems with internal controls or other negative surprises. Consider these statistics:

- According to a McKinsey Study, investors in North America and Western Europe will pay a premium of 14 percent for companies with good governance, as shown in Figure 1-1.
- The difference in stock market value for companies that had good internal controls versus those that did not is 33 percent.
- AMR Research predicted that companies would spend $29.9 billion on compliance initiatives in 2007 alone, up 8.5 percent from the previous year, indicating that GRC spending continues to grow as companies cope with the myriad challenges in this area.

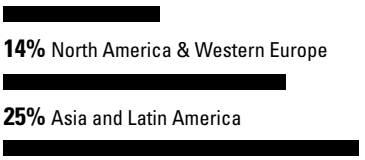
All of these forces combined led to the creation of the domain of GRC as companies realized that an ad hoc approach to meeting these demands was too expensive and actually increased risk for the companies because they couldn't mitigate issues they didn't know about.

The difficulty facing most companies right now is not how to meet these GRC challenges — the fact is, the forces that are driving increased attention to GRC are not optional for the most part and companies have no choice but to comply — but rather *how* to comply efficiently in a way that produces benefits. GRC shouldn't be just a cost that does nothing else for your business, but that may become your attitude if you want to be just good enough to barely meet minimum compliance standards.

Investors Reward Good Governance… and Penalize Poor Governance

Investors worldwide will pay a premium of 14% or more for shares in companies with good governance.

But companies with internal controls deficiencies experienced significant declines in their market caps:



McKinsey & Co. Global Investor Survey

2004 Disclosure Examples: Company/Market Value		Disclosure	% / Mkt Cap Decline
Adecco SA $12.6 billion	Jan. 12	Company delays financial statements. Internal control deficiencies	-38% $4.9 billion
Goodyear Tire & Rubber $1.7 billion	Feb. 11	Company has not yet completed the implementation of its plan to improve internal controls	-18% $320m
MCI $5.4 billion	Apr. 29	Material weaknesses – lack of systematci and reliable internal controls	-17% $935m
INVESTORS FINANCIAL $2.9 billion	Oct. 21	Material weakness discovered during review of internal controls	-16% $475m
FLOWSERVE $1.3 billion	Oct. 27	Material weakness in internal controls; two quarterlies overdue	-11% $152m

Figure 1-1: Rewards for good governance.

One way of thinking of GRC is to compare the process of managing a company to driving a car. When you drive a car, you have a certain set of rules that you are expected to abide by. You have to have a driver's license and insurance. Your car must be inspected for compliance with safety and environmental laws. When you are driving, you are encouraged by law enforcement and penalties to drive within speed limits and other restrictions. You may have your own rules about driving, such as never driving while talking on your cell phone in order to be as safe as possible. Other activities such as maintaining the car are up to you and various drivers will have different approaches. Some will change the oil more often than recommended or rotate tires frequently, some will use premium gas, and so on.

What has happened with GRC, to use the driving analogy again, is that the laws for everything related to driving got tighter and more restrictive and the penalties got higher. In addition, the rewards for driving efficiently and safely became much higher. So, you can now figure out how to drive just to keep out of trouble with external watchdogs, or you can figure out how to drive in a new more efficient way that better helps your business win in the marketplace, while still playing by all the rules.

GRC is a new management mentality. The bad news is that more work is required to comply with regulations. More testing and controls have to be in place and the organization has to be carefully designed. As exceptions to

policies occur, behavior must be checked and monitored. As people are promoted or job descriptions change, controls must be put in place so that compliance can be maintained. New forms of data must be captured and consulted. Risks must be proactively discovered while they are still small enough to manage. Without a doubt, this brave new world requires more work, and there is a shortage of trained people and expertise to carry it out.

The upside of GRC is that in addressing these issues systematically, the culture and performance of a company improves. In many ways, GRC is concerned with meta processes, which are those that look at the shape and flow of information in other processes in order to identify weak points. Controls and compliance are only one result of GRC: They put the C in GRC, if you will. When properly addressed, GRC helps identify ways that core business processes can be improved. Identification of risks also leads to discovery of opportunities. Governance processes can help create orderly ways to evolve a company, and improve program and change management across the board.

Getting Motivated to Make the Most of GRC

Although concern about GRC is growing, most companies that have engaged in a program of GRC are usually reacting to some pressure or concern that takes GRC from a necessary evil to an initiative that can really benefit the company if is executed thoroughly and efficiently. A serious approach to GRC may flow from any or all of these motivating forces that we discuss in the following sections.

Complying with financial regulations

New laws in the United States and in many other countries mean that if serious errors in financial reports are found, those responsible will face criminal prosecution. Section 302 of Sarbanes-Oxley says exactly this, and prosecutors around the nation have shown great eagerness to enforce this law.

It is not just American companies that are facing such dramatic penalties. See the "A global reaction to improve governance" sidebar later in this chapter for more on changes to GRC laws in other countries around the world. Governments of most of the largest economies have passed their own forms of legislation increasing the level of scrutiny about financial reporting and controls.

The driving force behind this regulation is the fear that inaccurate financial reporting will damage the financial system. Without accurate financial information, investors will have little to go on when making decisions about where

The march of the three-letter acronyms

The world of enterprise software has given birth to many Three-Letter Acronyms, called appropriately by yet another three-letter acronym: TLA. Here is a sample of the most common TLAs:

- Enterprise Resource Planning (ERP) software emerged in the 1990s to provide a complete financial model of a business along with tracking many other aspects. ERP was about closing the books faster and tracking the key financial and management processes of a business.
- Customer Relationship Management (CRM) software emerged in the late 1990s to give a name to software that tracked sales, service, billing, and other activities related to customer interactions with a business. CRM was about getting closer to the customer.
- Supply Chain Management (SCM) software emerged in the 1990s to track the flow of goods and manufacturing processes among a distributed network of partners working together. SCM helped manage increased specialization, outsourcing, and globalization.
- Product Lifecycle Management (PLM) software emerged in the 1990s to give a name to the processes related to creating new products, bringing them to market, and improving them. PLM was about helping increase the speed of product development.
- Governance, Risk, and Compliance (GRC) software emerged in the 2000s to automate controls to facilitate compliance with financial, environmental, health, and safety, and trade regulations, enforce internal controls, increase the efficiency of audits, identify risks, and employ proper governance procedures to keep all of these activities up to date and effective.

to place their money. If confidence drops too far, all companies, not just those who have engaged in bad behavior, will find it harder and more expensive to raise money. This is not the first time that such fears have been raised and reporting requirements have been tightened. Even the powerful tycoons of the Robber Baron era had bankers insisting on better accounting.

So, while compliance with regulations aimed at improving financial reporting and governance is really just one piece of the puzzle when it comes to GRC, fears related to such compliance are clearly the force that has driven most companies to action.

Failing an audit

There is nothing like failing an audit to spur companies to improve their GRC processes. In the wake of a failed audit, which must be reported in public financial statements, investors frequently lose confidence and sell stock.

Nowadays, audits can fail for more reasons than ever. Discovery of fraud or other bad behavior is of course the most dramatic reason. But in the face of

tighter regulations for governance and reporting, audit problems can include the lack of adequate controls, improper segregation of duties, insufficient oversight of the creation of financial reports, and many other causes. So even if nothing is wrong, you can fail your audit for not having sufficient documentation.

In the wake of a failed audit, reporting requirements skyrocket. Controls, which are detailed reports of various types of activity that must be cross-checked for problems, may have to be run on a monthly or quarterly basis instead of annually. New controls are usually introduced. Other sorts of testing to discover problems will also usually result. The work related to all of this new activity must be staffed either from inside a company or by personnel from an auditing or consulting firm. Either way, costs rise.

A global reaction to improve governance

Everyone talks about Sarbanes-Oxley (SOX), but it's certainly not the only law shaping governance today. Numerous countries have enacted legislation to improve governance. As with the United States, many of these countries have passed legislation in response to the outcry over corporate scandals. Although they differ by name, the laws passed by various countries have similarities, namely with regard to establishing internal controls and effecting improved financial reporting:

- **Japan: J-SOX:** On June 7, 2006, Japanese legislators passed the Financial Instruments and Exchange Law, part of which includes the so-called J-SOX requirements. The two main components of the J-SOX legislation are the "Evaluation of and Reporting on Internal Control for Financial Reports," which forces management to assume responsibility for developing and operating internal controls, and the "Audit of Internal Control for Financial Reports," in which a company's external auditor, aside from its regular auditing duties, must conduct an audit of management's evaluation of the effectiveness of internal control for financial reports. The J-SOX requirements took effect starting in April 2008.
- **Canada: Bill 198:** Bill 198, also known as C-SOX, became effective on October 1, 2003. Its formal name is "Keeping the Promise for a strong Economy Act (Budget Measures), 2002." This bill requires companies to "[create and] maintain a system of internal controls related to the effectiveness and efficiency of their operations, including financial reporting and asset control." It also requires companies to place internal controls over their disclosure procedures.
- **Australia: CLERP 9 in Australia:** In 2001, Australia passed the Corporations Act, which governs corporate law. In 2004, a reform to the Corporations Act was passed, called the Corporate Law Economic Reform Program (Audit Reform & Corporate Disclosure) Act 2004 (or CLERP 9). CLERP 9 aims to make sure that business regulation is consistent with promoting a strong economy, in addition to providing a framework that helps businesses adapt to change. Three entities were created by CLERP 9: The Financial Reporting Council, the Australian Stock Exchange's Corporate Governance Council, and the Shareholder and Investors Advisory Council.

- **England: Combined Code of Corporate Governance:** In England, as in many other countries, legislation has been enacted as a response to corporate scandal. Two of the most famous scandals were Polly Peck and Maxwell of the late '80s and early '90s. These scandals led to the creation of quite a few reports that dealt with many governance issues. One of these reports, the Hampel Report, led to the Combined Code of Corporate Governance (1998). Some of the areas the Combined Code covers are the structure and operations of a company's board, its directors' pay, accountability and audit, and the responsibilities of institutional shareholders.
- **India: Clause 49:** Clause 49 went into effect in December 2005. Its main goal is to improve corporate governance for all companies listed on India's Stock Exchange. Clause 49 focuses on issues that are already implemented in many other countries, such as establishing a board of directors and appointing a managing director who reports to the board, in addition to the creation of an audit committee. A revised Clause 49 was released on October 9, 2004. This revision covers many areas, including a clarification and enhancement of the responsibilities of the board and the director and a consolidation of the roles of the audit committee as they relate to controls and financial reporting.

The rising costs that occur after a failed audit are a powerful motivator for a company to automate its GRC processes so that controls and testing are much easier and cheaper.

Experiencing a rude awakening

Another sort of inspiration for improved GRC performance comes in the form of outside scrutiny. When auditors come in and start asking questions, sometimes companies discover that they don't really have their GRC issues under control after all. Usually this happens because people do not deeply understand the demands that laws and regulations are placing on them or the complexity of meeting those demands using their current software systems.

Scrutiny can also come from senior management, the board of directors, new employees, auditors, and so on. The problem with GRC and the reason that it has become a new TLA is that it can be hard and complicated to get right. Companies that lack the knowledge and expertise may think they are safe when they actually are not.

Going from private to public

The imminent conversion of a company from a private form of ownership to a public form can be another driver of increased attention to GRC. An Initial Public Offering (IPO), in which a company sells stock to the public for the

Jail, schmail

The drumbeat of GRC consultants stating that "we'll keep you out of jail" has too long defined the conversation about GRC. It's time for a reality check.

Jail is a remedy for people who are engaged in criminal activity. But if you're entering a GRC program to stay out of jail, you're missing the point. The point of GRC is to run your business better, expand your consciousness of what is going on, and provide employees with guidance about what they should be doing and to find out when they're not doing it.

You can apply that knowledge to all sorts of areas: governance, risk, compliance, trade, environmental, data privacy, and much more. If you do it right, GRC can help you run your business better than ever before, gain competitive advantage, and increase the rewards to you and your shareholders.

From a shareholder perspective, which is worse: a CEO going to jail or an entire company running itself on stale data?

first time, is a common way for a private company to become a public one. But other events such as selling bonds or issuing other forms of debt can also initiate the same requirements to meet higher levels of reporting.

Private companies also seek to improve their GRC processes if they may be up for sale to public companies that have to meet more stringent levels of governance and reporting. Whether you're looking at a merger or acquisition or taking a company public, having all the ducks in a row, so to speak, can make the acquisitions process much smoother and can also make the difference between controlling the timing of an IPO or playing catch-up to try to get things in order.

On the other hand, even private companies can benefit from implementing the best practices highlighted by SOX. Private companies with government contracts get a favorable reaction from the government when they implement best practices based on SOX. There's certainly no harm in improving internal controls and corporate governance, and the benefits can be very real both in terms of clean financials and process efficiencies.

Managing growth

Smaller companies that are on a dramatic growth curve frequently use a GRC implementation as a way to make sure that as new employees are quickly hired, threats to the organization's financial health do not occur. With appropriate controls and tests, management can rest assured that the company is not at risk as more new people take over key tasks.

Smaller companies generally have more issues with segregation of duties for obvious reasons. Segregation of duties requires dividing key steps among employees to help prevent fraud that could take place if one person did all the tasks. But with fewer employees, there is less specialization and a single person may be doing many more tasks than in a larger company.

One common misunderstanding is that implementing GRC means that all potential conflicts are eliminated. Even in the largest companies, this is almost never the case. Usually, some employees are able to do things that might result in fraud. Such potential conflicts can be handled by adding controls and tests that reveal any bad behavior.

Taking out an insurance policy

When new owners arrive to take over a company, implementing GRC is one common way to make sure that everything is operating properly and that nothing fraudulent is taking place. GRC is like added insurance for the new owners: Adding the controls and testing that is part of a thorough GRC implementation provides added assurance that the financial management of a company is taking place in a proper way and that the condition of the company is accurately conveyed by its accounting reports.

Managing risk

Companies that have had a series of nasty surprises often improve GRC processes and automation as a way to create an early warning system to identify and manage potential operational risks. Unforeseen risks can lead to punishment in the markets as investors worry about what problems might be next.

As this chapter has noted, it is a mistake to think of GRC only in financial terms. Risks that have dire financial consequences can arise from a multitude of operational factors that never show up on a balance sheet. For example, in a manufacturing plant, what if spare parts inventory for a key piece of equipment drops to dangerously low levels? If someone notices this, how can they go on record to make sure that the significance of the risk is understood and that management knows that something must be done to avoid a huge problem? The risk management processes of GRC provide just such a solution.

Reducing costs

The desire to cut costs related to GRC is another major driver of GRC automation. In the mad rush to comply with Sarbanes-Oxley in 2004, many compliance activities were performed manually. Information was gathered,

organized in spreadsheets or other simple ways, and then used to make sure that the company was complying with all requirements.

While this sort of manual work was inevitable the first time around, and perhaps even beneficial in that it gave those involved a hands-on understanding of what sort of work needed to be done and information needed to be assembled, it was not efficient.

Given the shortage of personnel trained in GRC and the expense of using external consultants and auditors to perform reporting and analysis related to controls and testing, many companies are seeking to implement GRC as a way to increase automation and cut costs. Some companies have reported reductions in auditing costs of more than 20 percent.

Struggling with the high volume of compliance

Risk goes way beyond financials and so does compliance. Globalization means that goods may be sourced from just about anywhere and shipped anywhere, and the compliance requirements for moving these goods are significant: each cross-border trade can involve as many as 25 different parties and generate 35 documents that must be tracked and saved. Furthermore, security issues have made the "anywhere" part of this more difficult as well; there are about 50 denied persons lists — lists of undesirable persons and companies that governments forbid shipping goods to — that must be checked before goods are shipped.

Environmental regulations are also increasingly the focus of compliance. The number of environmental regulations companies must comply with is constantly growing, both at the state and national level, particularly relating to hazardous substances. In many cases, the sheer volume of compliance activities forces automation because no other approach is feasible.

Introducing the GRC Stakeholders

No matter what the motivators and how much automation you may apply, the essence of GRC is to change the hearts and minds of the people in a company. The responsibility for GRC enforcement and implementation is spread across a variety of different stakeholders, each of which plays an important role. Understanding the interactions between these stakeholders is a key element of a successful program of GRC improvement.

GRC stakeholders inside a company

Like every other major trend affecting business, increased attention to GRC concerns is having its effect on the organizational chart. Of course, the ultimate responsibility for all corporate issues resides with the board of directors and the CEO, and then devolves down through the organization. At most companies, the operational responsibility for implementing a program for improving GRC performance resides with the COO or CFO. The consequences of inadequate attention to GRC processes are so extreme that interest from senior management is at an all-time high.

The need for effective management of GRC has led to the creation of a new set of titles that may include any of the following:

- Chief Compliance Officer, Vice President of Compliance
- Chief Risk Officer, Vice President of Risk
- Chief Sustainability Officer, Vice President of Sustainability
- Manager of
    - SOX
    - Compliance
    - Risk
    - Sustainability
    - Trade Management
    - Environment, Health, and Safety

Some analysts recommend that companies keep any organization dedicated to GRC as small as possible. From this point of view, GRC should be something for which every line of business is responsible. The creation of a separate department dedicated to GRC is an invitation to empire building. After a department dedicated to any specific purpose is created, it tends to grow. The ideal way to implement GRC is to make compliance efficient and easy through controls, training, and automation so that improved business processes make the process easy, a part of everyone's day-to-day work, instead of creating a large cost center.

GRC stakeholders outside a company

Investors and shareholders have perhaps the most to lose monetarily from failures of GRC processes. When a stock price drops after a company reports an audit failure, a material breach of compliance with regulations, or any other sort of negative event that could have been foreseen, investors are demonstrating their profound concern.

Besides investors, the other important external groups are institutions inside and outside of government that set rules that must be followed. This group includes all of the following types of organizations:

- Legislative bodies that make laws that must be complied with.
- Government agencies responsible for carrying out laws, such as OSHA, the EPA, U.S. Customs, and many others.
- Financial regulators that set standards for financial reporting, such as the Securities Exchange Commission, Financial Accounting Standards Board, Federal Reserve, Bank for International Settlements, and others.
- Non-governmental Organizations (NGOs) charged with setting policies that govern how business is done, such as the United Nations.
- Trade organizations such as the World Trade Organization, World Intellectual Property Organization, NAFTA, CAFTA, and others.
- Auditing firms that certify the correctness of procedures and policies used for financial reports.

This list of stakeholders is constantly changing as new issues arise and new laws and regulations are created to address them.

Understanding GRC by the Letters

So far in this chapter, we've treated GRC like a large black box: a mysterious container full of improved processes and software for automation. Now it is time to open that box and look inside at all the moving parts. The challenge in moving to a more detailed discussion of GRC is that the meaning of the terms and the actions required are different depending on the nature of the business. GRC activities at a stock brokerage firm will be quite different from those at a chain of grocery stores, for example, although the goals at the highest level are the same.

This section breaks down GRC into its component parts by looking at the meaning of each of the three words that make up the acronym: *governance*, *risk*, and *compliance*. The challenge here is that these words are general terms as well as terms of art applied to GRC, so we start our discussion by separating the informal meanings of the terms from the precise way these words are used with respect to GRC.

Governance

Governance is a general term. The way that a board of directors works with a CEO is a form of governance, for example. The governance in GRC is that which is exercised by the CEO on down. How are you going to do what you must do to execute on a strategy? How is the CEO making sure that the right policies and procedures are in place to run a company? How are those policies communicated? What sort of checking is done to make sure that the policies and procedures are being followed? How are the policies and procedures updated? What controls are in place? How can methods of checking and confirming that policies are being followed be improved?

Risk

The word *risk* is the trickiest of the three that make up the GRC acronym. All of GRC, for example, can be seen as an exercise in understanding and controlling the risk of running a business. So a program of GRC improvement helps reduce the risk of failing to comply with regulations for financial reporting, trade, environmental protection, or safety. GRC also deals with the risk of not having adequate governance structures to keep a company under control and effectively managed. Every business strategy runs certain risks that can be identified at the outset and must be monitored. There is also the risk of not identifying operational risks that may have significant impact on a business early and dealing with them adequately. The R in GRC includes all these risks, in fact, any risk the business faces.

Compliance

Compliance is the term that has a general meaning that is closest to the way it applies specifically to GRC. Compliance in general means that you are satisfying a set of conditions that has been set forth for you. Compliance implies that someone else has set those conditions up and that you must meet them. That's exactly what's going on in GRC. Most of the time, when people talk about compliance, they are referring to external standards for which compliance is mandatory. The word compliance also sometimes refers to internal standards as well.

Defining the C in GRC as standing for *controls* can broaden the discussion. Compliance is what we have to do, and controls are the way we do it. Furthermore, controls are a way to monitor that the business is compliant, and also efficient and orderly in every way.

Figure 1-2 shows the way that the three core activities of governance, risk management, and compliance interact.

Figure 1-2: Interaction between processes for governance, risk, and compliance.

Figure 1-2 shows GRC from the top down. Governance guidelines, which are the policies and rules of the game for a company that explain how the company will be run to best meet its obligations and pursue the business strategy, are set forth by senior management. The operational executives then carry out programs and put in place controls that ensure compliance, frequently with the help of consultants or auditors who are expert in applying GRC. Risk management results in the creation of mechanisms so that risks can be brought to the attention of senior managers who then take steps to reduce them.

So although Figure 1-2 shows a top-down structure, in most companies, GRC is actually implemented from the bottom up, like this:

1. The company puts in place controls to make sure that compliance requirements are satisfied so that no laws or regulations are violated.
2. After the controls are in place, which may take a year or more to achieve, the next task is to analyze what has been done to make it more efficient and effective and to reduce costs associated with compliance.

   At this stage processes for governance may begin to be developed as internal policies are added to external requirements and the company looks at its compliance activities from the top down.

Risk management processes may be added at any time during this cycle, depending on how worried a company is about risks connected to a particular strategy or about unforeseen risks. With this cycle in mind, in the next few sections, we explain the activities involved in each area of GRC in greater

detail. In preschool, you may have learned letters by remembering that A is for apple: The same approach can be taken with GRC. We take the bottom up approach in our explanation and work through the acronym from right to left.

C Is for Compliance: Playing by the Rules

The goal of the compliance process is to make sure that a company meets or exceeds all of the demands that are placed on it by external institutions that make laws and regulations for various purposes. Compliance is also concerned with self-inflicted rules; in other words, policies related to how a company does business. Financial compliance is the one that has gotten the most attention in the past couple of years, but trade management and environmental, health, and safety compliance are also always key concerns. These areas are all interrelated and provide companies a set of guidelines to follow from a perspective of best practices and processes. Each of these areas will be covered in detail later in this section.

Some regulations require that reports of activities are created and may set thresholds for acceptable financial ratios or amounts of emissions, for example. Others require that a company's processes have a certain shape or follow certain guidelines so that certain types of bad behavior become impossible or extremely difficult. But by far the most frequently mandated item from a compliance perspective is the mandate that a company have sufficient controls to detect bad behavior. A complete grasp of what controls are and how they work is key to a complete understanding of GRC.

Controls: Mechanisms of compliance

Controls are the means by which bad behavior or violations of policies are discovered. Controls also provide companies with an alert mechanism for highlighting what processes are working well and which areas need to be improved. By finding out what's working and what's not, companies can optimize all their processes through the enterprise.

Some controls are *preventative*, meaning that they stop you from doing things that are not allowed. Preventative controls are frequently part of access control, which is the discipline of allowing people to have access only to transactions and capabilities that they need to do their jobs and to limit the potential for bad behavior. Access control is key to managing segregation of duties, which is one of the most important mandates of Sarbanes-Oxley. See Chapter 5 for more information about segregation of duties.

Although stopping people from bad behavior is a great idea, preventative controls are too blunt an instrument to enforce complex policies that may prohibit actions that take many steps to complete. Most of the controls that are used to enforce policies in a company are *detective controls*, which analyze what has gone on in a company and reveal policy violations or bad behavior after it has happened. Although in some ways it seems like creating a system that makes bad behavior impossible is preferable, in practice, the processes in a business are too complex and fluid to be automated in such a rigid way. When implementing policies and enforcing them with detective controls, you never stop people from doing what they need to do to keep the business running. You do, however, detect the problems after they occur and then come up with remedies of various sorts to mitigate the problems and prevent them in the future. *Mitigating controls* are those controls that are put in place to fix any problems created by violations of policies. Mitigating controls are descriptions of steps that need to be taken to fix problems.

Detective controls can either be automated or manual. For a *manual control*, someone may have to scour through the logs of various types of activity to find certain types of transactions and record them in a spreadsheet. Then the collected transactions are analyzed to see if any of the transactions have violated a policy. *Automated controls* gather the information and check for the violation automatically. Automated controls can also generate alerts and cases that can be assigned to the appropriate manager for remediation. One of the key methods for making GRC processes more efficient is through the application of automated controls. Given that most companies have around 500 controls in place, improving the efficiency of controls can mean significant savings. (For more on access control, see Chapter 6; turn to Chapter 7 for more on internal controls.)

Controls are determined by the direction provided by corporate governance and risk management and then are applied to the most important processes of the enterprise. One common control is to check the credit of each new customer before doing business with them. A control could take the form of looking at each new customer record and then examining activity to see if a credit check was performed. If new customers have been created without credit checks being performed, a mitigating control may need to be executed, perhaps to perform the credit check after the fact. Then the control may analyze why the credit check was not performed. Perhaps the problem is systematic, resulting from inadequate training, for example. Maybe the people creating new customers did not know that a credit check was required. Perhaps the problem was that the system used to check credit is unreliable so that credit checks cannot always be performed. Whatever the reason, the control can discover a problem that must be dealt with to comply with a policy or regulation.

Some controls are run once a year; for example, to check whether policies for capitalizing equipment are followed. Other controls may be run once a quarter or once a month. One of the things that usually happens when problems are discovered in an audit is that controls are run more frequently. If the controls are manual, this means that someone must be doing a lot more work,

which can drive up auditing and personnel costs (and the cost of doing business). Replacing manual controls with automated controls is one way to allow controls to be run more frequently — in some cases, continuously — without large additional costs. That way, if 1 in 100 transactions violates a control, an automated control will catch it every time without incurring the cost of checking the 99 transactions that did not violate the control. A manual control that tests every transaction would find such a problem, but the more common approach — sampling transactions — is unlikely to find needles in haystacks. Automated controls save money, run 100 percent of the time, and allow you to practice exception management.

In the process of designing, applying, and analyzing controls in a business, you develop a deeper understanding of the processes of your business. Problems discovered by controls can lead to the redesign of processes to better meet both business and compliance goals. To get the most out of GRC, the insights gathered in compliance activities must be shared with managers in each department so that compliance can become part of the process of continuous improvement.

Domains of compliance

The sorts of controls just described are used in numerous domains of compliance: financial management, global trade, and environmental, health, and safety. In each of these areas, different external regulators have set forth increasingly complex rules and regulations. Proof of compliance with these regulations may be required in the forms of controls, reports, and certifications to the veracity of reported information. The section below summarizes the sorts of compliance that are required in each area. For much more information, see the following parts of this book:

- Financial compliance is covered in Part II.
- Trade management is also covered in Part II.
- Environmental and safety concerns are covered in Part III.

In addition to these traditional domains of compliance, some newer compliance domains also fall under the GRC umbrella:

- Privacy regulations
- Risk management regulations
- Sustainability
- Internal policies

In the following sections, we discuss each of these domains in detail.

Financial compliance

Financial compliance these days is dominated by the regulations that have been introduced by Sarbanes-Oxley. Section 302 of the law makes it a crime to certify financial statements that have material errors. Section 404 requires strict segregation of duties to prevent various forms of bad behavior including fraud, inaccurate reporting, and other forms of malfeasance.

Section 302 requires that CEOs and CFOs literally sign on the dotted line on annual and quarterly reports and certify that the information is true. Behind that signature are many other levels of signatures of everyone in the chain of command, stating that they vouch for the numbers they provided for this report. Controls designed to monitor key processes are one of the ways that executives and managers feel comfortable putting their signatures on these reports: Controls help to verify that the numbers are accurate and not inflated.

If a CEO knows that processes like order-to-cash, revenue recognition, and procure-to-pay are all being monitored closely through a comprehensive set of controls, the CEO (and those under him or her) can feel comfortable certifying that there is no fraud or inaccuracies in financial reports. If errors do show up, everyone involved will be more understanding if a full set of compliance and information quality procedures are in place and diligently enforced.

Section 404 is handled through putting access control mechanisms in place. When someone is given access to a computer system, a role is usually assigned to them. That role has a set of permissions that grants that user access to a certain set of transactions. In a modern computer system like SAP ERP, for example, there can be more than 20,000 transactions and more than 100,000 data elements. Each company has hundreds of roles in place. It is impossible to manually check that the roles assigned to any one individual do not grant access that would violate any reasonable segregation of duties schemes. Depending on the nature of a business, a company may have to provide other forms of reporting, such as levels of capital for banks or other indicators of financial health.

Modern GRC systems help automate the process of implementing, running, and analyzing controls, performing segregation of duties checks, and creating regulator reports of all kinds.

Trade management compliance

Compliance with trade management regulations was never simple and has only become more complex in the post-9/11 era. If you're doing business with someone overseas, you must document the answers to the following sorts of questions:

- Who is it acceptable to do business with?
- Which goods can be sent to which countries?
- What are the limits on amount of goods sent to each country or buyer?

- What goods qualify under trade agreements?
- How must goods be labeled?
- What information is required to clear customs?
- Is a license required?
- Is a letter of credit required?

Each country has its own regulations. For example, worldwide there are approximately 50 different lists of denied persons or companies that countries prohibit sending goods to. Many of these lists change daily. Although U.S. exporters are mainly concerned with the lists of denied persons from a U.S. perspective, best practices state that they should also check the lists for the countries to which they are shipping the goods. Also, governments are starting to use more advanced methods of providing information and are requiring electronic submission of global trade documents. Globalization and outsourcing mean that more and more goods are moving across borders. When products are shipped, regulations of the receiving and sending countries must be satisfied as well as any countries that the goods pass through.

Companies at one time left many of these tasks to the shipping and freight-forwarding companies. But now compliance is so challenging and the penalties so severe that this is less often a viable solution. The latest trade management systems help automate these activities as much as possible through integration with internal systems like ERP (Enterprise Resource Planning) and SCM (Supply Chain Management) and external sources of information.

Environment, health, and safety compliance

Environmental, health, and safety regulations are constantly moving forward as new dangers are identified and new concerns arise. OSHA and the Clean Air Act in the United States, the RoHS act and REACH acts in Europe, and standards for labeling of hazardous materials, are just a small sample of the sort of regulations in effect.

For example, for companies that create and ship hazardous materials, labeling requirements differ throughout the world, as do requirements for the data sheets that accompany such materials.

Risk management compliance

Although laws regarding risk management are not yet mainstream compliance requirements in the U.S., risk management is increasingly becoming a compliance issue as well. Switzerland and Germany already have laws mandating risk management. In the U.S., official recommendations indicate that compliance for risk management may not be far away: the U.S. Amended Sentencing Guidelines state that organizations must take reasonable steps to ensure that their compliance and ethics programs are followed, including monitoring and auditing to detect criminal conduct and to evaluate periodically the effectiveness of their compliance and ethics program. Although risk management is

not explicitly stated in the guidelines, what is required to meet them is basically, in fact, a systematic approach to managing and monitoring risks. Also, the Public Company Accounting Oversight Board (PCAOB) and the Securities and Exchange Commission (SEC) recommends a top-down, risk-based approach to organizations' SOX compliance requirements.

Data privacy and security compliance

The problem of identity theft is driving increased regulation as well, both in the areas of data privacy and computer security, which go hand in hand in protecting sensitive data. Regulations are on the rise in this area, whether it's laws regarding how sensitive data must be protected or laws that kick in if a security breach has occurred (for example, the California Security Breach Notification Law). In the healthcare industry, HIPAA has strong implications for how data is handled. The COBIT framework helps companies organize their compliance in this area; Chapter 14 covers the important topic of IT GRC.

Sustainability reporting

A new horizon in this area is the domain of sustainability, which doesn't yet fall in the realm of compliance, but one day might. Companies are increasingly being asked to demonstrate that their operations do not have long-term damaging effects on the planet and that they practice good corporate citizenship. The United Nations releases a list of 230 sustainability indicators that companies may one day be required to report on. Chapter 13 discusses the topic of sustainability.

R Is for Risk: Creating Opportunity

Risk management is the process of uncovering what *could* go wrong for the express purpose of making more things go right. All strategies and all opportunities worth pursuing involve risks that must be monitored and managed. Racecars win not just because of their gas pedal but also because of their brakes, which help drivers deftly maneuver around corners and other obstacles. In the same way, risk management can help companies identify potential pitfalls and thereby optimize their opportunities for success.

Many types of operational risks don't appear on the balance sheet but can have disastrous consequences. Risks in this category include such hazards as

- Environmental catastrophes
- Difficulties with integration of acquisitions
- An aging workforce
- Extreme weather
- Currency fluctuations

- Kidnapping
- Terrorism

For example, if a key supplier is going to be taken over by a competitor, the sooner a company knows about it, the better. Or perhaps, a major customer has indicated they are in big financial trouble and may cut back on orders. Or, what if replacement parts for a critical piece of equipment are no longer being produced? A well-run company has a way for its employees to identify such risks and raise the alarm so that the risks can be prioritized and mitigated.

Unmanaged risks increase the potential for unpleasant surprises. Thinking that risk management is only about catastrophic risks is a mistake. A series of unanticipated smaller risks can have an equally devastating effect, especially if they cause targets for financial performance to be missed, even by a small amount.

Risk management, though it initially sounds negative, has great potential for helping companies maximize their opportunities. Reporting mechanisms to raise alerts about risks may also be used to identify opportunities. When done properly, risk management can be like a crystal ball that helps you get a vision of the future, tweak it according to your strategy, and make that improved vision come true.

G Is for Governance: Keeping Focused and Current

Governance is about the big picture, about steering a company in the right direction and evolving policies, procedures, and processes as needed. Governance is about how you are doing what the strategy of your business demands that you do. Governance is about establishing the larger goals, the top-down perspective that organizes compliance and risk management activities as well as everything else a company does. Governance is also about how the data gathered by GRC processes is analyzed and used to improve a business.

At the highest level, governance is about steering the corporation: making sure that a company is selling the right products in the right markets. Governance exists to translate the strategy set by the board of directors and CEO into the actions that will bring that strategy to life.

The first step most companies take with respect to GRC is to put in place controls that ensure the firm is complying with external requirements. But after that has been accomplished, the sort of self-governance shown in Figure 1-3 becomes an issue.

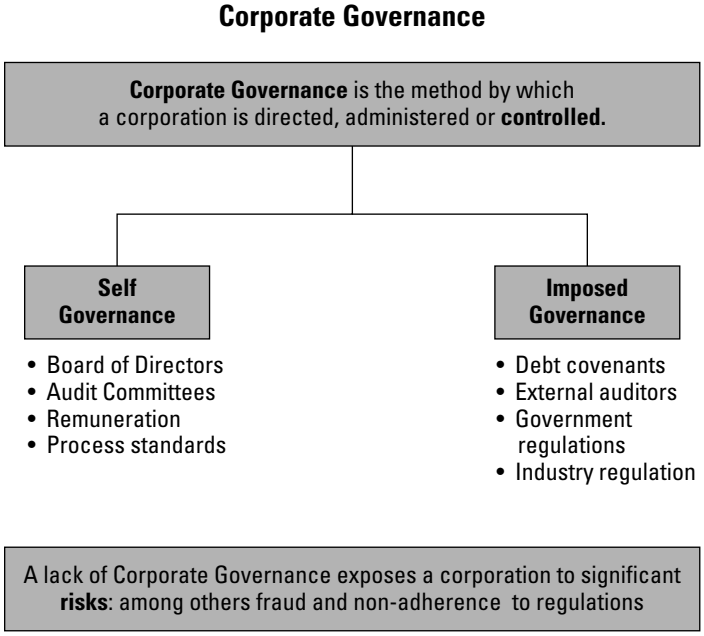


Figure 1-3: The three kinds of governance.

Self-governance means adding policies, procedures, and controls to enforce them to those already imposed by external parties. Self-governance helps create a continuous feedback loop of information to improve the operations of a company and to make sure that any important operational processes take place as desired by the board and CEO.

One of the most important governance activities is to look at the existing set of controls for both imposed and self-imposed governance and ensure that they have the proper scope and effect. In performing this analysis, a company frequently gains insights into how to redesign its processes to increase efficiency and better align them to corporate goals. After new ideas for improvements have been discovered, they must be implemented in order to take effect. In other words, governance, when properly implemented, helps guide the evolution of a company. For this reason, there is a natural link between governance and program management.

Hitting the Audit Trail

Increased attention to GRC has been a boon for auditing firms as companies have hired them to help make sure they are complying with Sarbanes-Oxley and other regulations. Auditors have been asked to help design and implement controls and to perform other forms of testing to ensure compliance.

Most auditing activity involves examining the transactional record of a company that is kept in various sorts of audit trails that record corporate activity. When this work is performed manually, it can take an enormous amount of time to carry out. One of the goals of most GRC improvement programs is to automate as many controls as possible, which means that audits can become more efficient. This can mean a reduction in certain kinds of auditing fees, but it also means that auditors can spend more time on higher-value activities. With more automation, the costs of audits drop but the benefits of audits rise.

Designing Your Approach to GRC

Each company approaches GRC differently depending on its needs and circumstances. Some firms find that focusing on compliance is all they want to tackle. Firms in this group may not have trade management or environmental, health, and safety problems to deal with and may feel that their existing processes for identifying risks are working adequately. Other companies may feel they have a good collection of compliance processes in place already and just want to improve their risk management.

But no matter where a company started from and where it is at now with respect to its GRC processes, the cost of compliance is large and growing. Some analysts estimate that companies spend $1 million on compliance for every $1 billion in revenue. Eventually, the board of directors and CEO will want to reduce GRC costs, or maybe another of the motivators we mentioned earlier in this chapter kicks in. That's when a program of GRC improvement begins.

After the rush to clean up

The most common pattern that leads to a desire to reduce GRC costs was caused by the rush to comply with Sarbanes-Oxley in 2004 (see Figure 1-4).

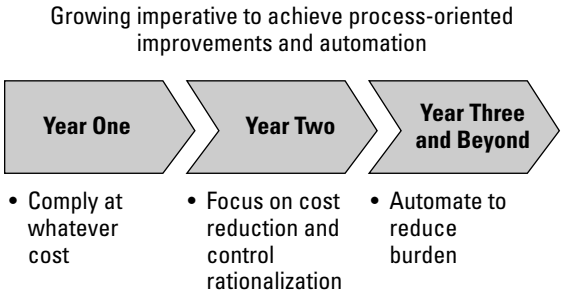


Figure 1-4: The phases of GRC adoption.

- In 2004, companies went through the sprint phase. Risks were identified and managed with appropriate controls. Roles and user access were cleaned up.
- In 2005, the marathon phase began. Companies focused on staying clean and lowering the costs of compliance.
- In 2006 and beyond, companies started to focus on automation to bring costs down to the lowest level possible.

Another, no doubt oversimplified, way of putting it is that companies rushed to get clean regardless of cost, and then sought to stay clean as cheaply as possible.

Stages of GRC adoption

Observers and analysts watching the progression of GRC adoption have identified four stages of growth and maturity that companies move through as they improve their GRC processes: reacting, anticipating, collaborating, and orchestrating. As shown in Figure 1-5, the first step is *reacting*, which is the rush to get things done.

The second step, where most companies are now, involves *anticipating* needs and increasing automation. The third step involves higher levels of *collaboration* in which GRC awareness is propagated throughout an organization. In the fourth phase of GRC adoption, a company seeks to better *orchestrate* and optimize its activities based on greater visibility.

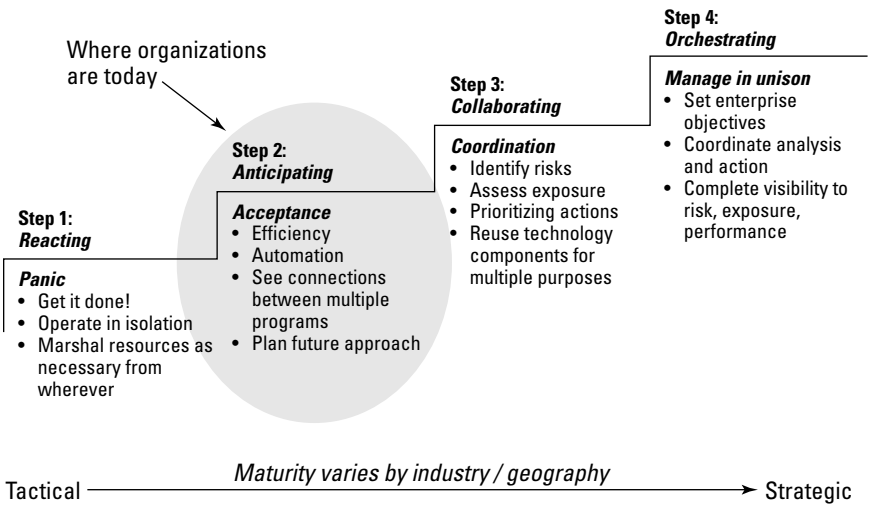


Figure 1-5: Stages of GRC adoption defined by AMR Research.

As companies grow in their maturity, they cut costs for compliance and auditing, increase the scope of activities that are monitored by GRC processes, and make better use of existing systems for GRC purposes.

What GRC Solutions Provide

Companies have found that the ad hoc approach that was used in the sprint to get clean is expensive and unwieldy. Manual processes that use spreadsheets to gather and analyze information work to establish compliance, but drive costs up as the same manual work is repeated again and again. Executing controls through armies of testers has the same problem. With an ad hoc approach, there is no common repository for GRC information and little benefit from GRC activities. An integrated approach to GRC allows for risks from one side of the business to be reviewed by the other side, helping to quickly build a corporate knowledge base of best practices. The benefits of an integrated approach to GRC can best be accrued by implementing an integrated GRC solution.

For example, sometimes companies briefly give super-user control of their systems to people who otherwise don't have that level of access, perhaps for year-end processing or because key personnel are on leave. Such access must be tracked and later carefully revoked. The ad hoc approach to access control can get you clean, but it doesn't keep you clean: It's hard to remember to revoke that access after the stress of year-end processing has passed. Smaller companies take the approach of having their audit partners run a one-time testing to identify access control risks annually. The problem is that this provides only a snapshot, and without a GRC solution to help monitor this on a day-to-day basis, problems may go unnoticed for nearly a year before they are uncovered.

Vendors of GRC software such as SAP have created products that are aimed at making GRC processes as efficient and inexpensive as possible. Companies are increasingly adopting GRC solutions because doing so saves money through automation and provides a consistent context for management of GRC processes. Using GRC software is especially advantageous in today's environment in which there is a shortage of people with GRC skills and experience.

GRC solutions provide a common language and ready-made policies and controls that are built to work with the systems you have in place. A large part of the value of GRC systems comes from the content that such solutions provide. For example, a good global trade solution should come with real-time checks of denied parties lists and a way to generate the proper customs documentation to ensure that goods cross borders as quickly as possible.

Integrated GRC systems not only have a system for managing access control but they also have rules that take into account the thousands of specific transactions inside an ERP system so that segregation of duties conflicts can be avoided. In addition, GRC systems not only have systems for automating the collection of information and the analysis of that information for controls, but they come with a large set of commonly needed controls that are ready to implement.

Perhaps the largest benefit of GRC systems is that they come with a step-by-step approach of the sort shown in Figure 1-6 that is proven through the experience gathered at numerous companies.

The general approach of one component of SAP's solution, SAP GRC Process Control, is to follow these steps:

1. **Document the control environment.**

   What are you doing? What are your processes? Where are the risks?

2. **Test: Implement the process and access controls needed to address the risks identified.**
3. **Remediate: Resolve exceptions found by the controls.**
4. **Analyze: Use the information gathered to gain a deeper understanding of the business.**
5. **Optimize: Improve both GRC and business processes as insights are gathered.**

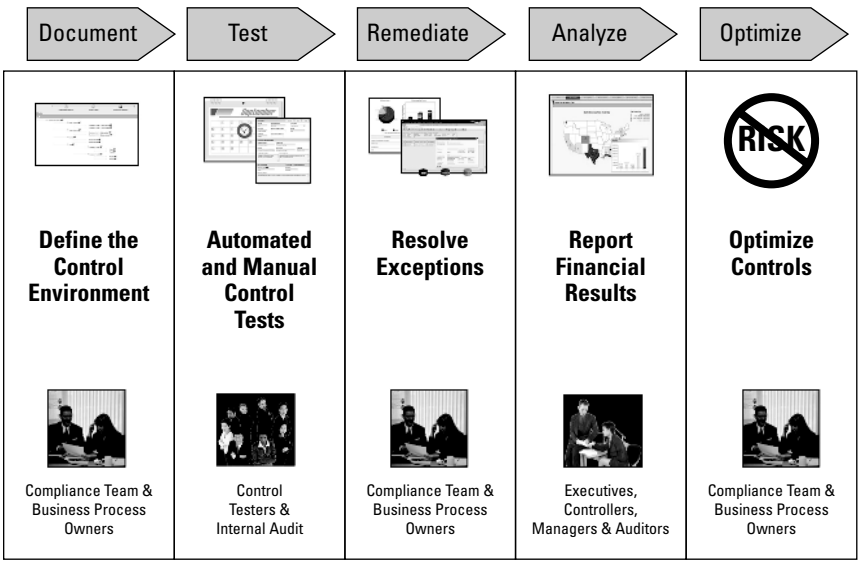


Figure 1-6: The steps to GRC implementation.

Systematic application of a GRC solution leads to a process that constantly deepens management's understanding of what is going on in a business and increases their confidence that risks are being managed. Figure 1-7 shows how this leads to a closed-loop system of constant improvement of GRC processes.

With such a process of continuous improvement in place, companies get the most important benefit that they are seeking from GRC—the peace of mind that comes from knowing that financial information is accurate, risks are being managed, regulations are being complied with, and that the probability of nasty surprises is as low as it can be.

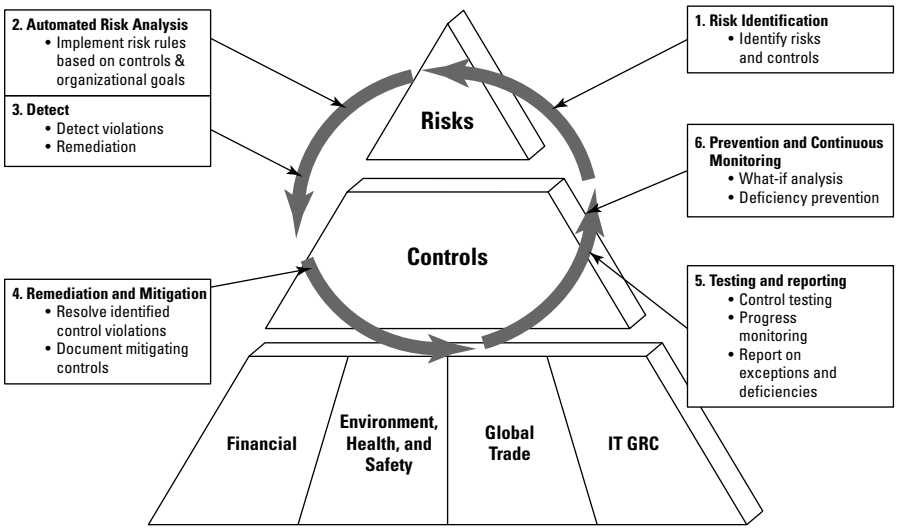


Figure 1-7: A closed-loop process of GRC improvement.